



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,811	01/31/2001	David Aro Bruton III	5577-223	2267

20792 7590 10/15/2007
MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER

TRUONG, LAN DAI T

ART UNIT	PAPER NUMBER
----------	--------------

2152

MAIL DATE	DELIVERY MODE
-----------	---------------

10/15/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

OCT 15 2007

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/773,811
Filing Date: January 31, 2001
Appellant(s): BRUTON ET AL.

D Randal Ayers
Reg. 40,493
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04/25/2007 appealing from the Office action
mailed 03/20/2007

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

Claims 1-9 and 14-28 stand final rejected. Claims 10-13 have been cancelled.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

U.S. 5,548,649 Jacobson 03-1995

U.S. 6,366,912 Wallent et al. 06-1998

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim rejections-35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-9, 14- 28 are rejected under 35 U.S.C 103(a) as being un-patentable over Jacobson (U.S. 5,548,649) in view of Wallent et al. (U.S. 6,366,912)

Regarding claim 1:

Jacobson discloses the invention substantially as claimed, including a method, which can be implemented in a computer hardware or software code for selectively allowing access to a plurality of resources in a network, the method comprising:

Receiving a request originated from a user of a multi-user system to transmit a message via the multi-user system over the network to one of the plurality of resources: (Jacobson discloses a security system supports for communications between secure zones networks (e.g. 108-1, 108-2, 108-3) those bridging by secure bridges, see (figure 1; abstract); wherein each of secure zones network comprises group of host computers e.g. mainframes, supper computers and

file servers...etc. see (column 3, lines 9-18). Jacobson's system can be pictured as communications between different secure zones networks, thereby one of secure zones network comprises mainframes, obviously the mainframes are often shared by multiple users connected to the mainframes by terminals; the other secure zones network comprises "file servers" that shares functionality with "resources" as claimed, see (column 3, lines 9-18). Jacobson further discloses a forwarder comprised in the bridges receives and determines authorization for "packet data" which shares functionality with "the message" as claimed by associating source IP address comprised in packet data with IP address of secure zones in identification tables to determine if the data packet is authorized, and then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding the encrypted packet data to desired/selected secure destination: column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

each of the plurality of resources has been assigned to one of a plurality of security zones: (Jacobson clearly discloses distinct security zones networks (e.g. secure zone 108-03, 108-01, 108-2) associated with groups of host computers those could be file servers, or mainframes, or super computers: column 3, lines 42-67, 7-18; figure 1)

identifying a one of the plurality of security zones that is associated with the one of the plurality of resources: (as similar to rejections addressed above, Jacobson disclose technique of sparing source IP address comprised in packet data with IP addresses of secure zones in local/remote secure zone Host ID tables to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt

the packet data prior forwarding it to “desired/selected secure destination” which shares functionality with “resource” as claimed: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1; column 3, lines 42-67, 7-18; figure 1)

determining if the user of the multi-user system is authorized access to the identified one of the plurality of security zone: (Jacobson discloses a forwarder comprised in the bridge determines authorization for data packet by associating “source IP address included in data packet” which represents for user identification of the user of the multi-user system as claimed with IP addresses in secure zones in identification tables to determine if the data packet is authorized to be forwarded to other secure zone networks; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data for forwarding to “desired/selected secure destination” which shares functionality with “an identified security zone”: column 7, lines 19-67; column 8, lines 1-48, 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 15, lines 1-67)

forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the identified one of the plurality of security zone: (as similar to rejections addressed above, if source IP address included in data packet is determined as authorized, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the data packet prior forwarding it to “desired/selected secure destination” which shares functionality with “an identified security zone”: column 7, lines 19-67; column 8, lines 1-48, 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 15, lines 1-67)

However, Jacobson does not explicitly disclose level of security sensitivity of the resource

In analogous art, Wallent disclose method for grouping web servers into secure zones based on levels of security: (abstract; column 2, lines 36-49; column 3, lines 20-27)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wallent's ideas of grouping servers into secure zones base on levels of security with Jacobson's system in order to increase security of communication system, see (column 2, lines 37-49)

Regarding claims 14 and 19:

Those claims are rejected under rationale of claim 1

Regarding claim 25:

Jacobson discloses the invention substantially as claimed, including a system, which can be implemented in a computer hardware or software code for selectively allowing access to a plurality of resources in a network, the method comprising:

A data processing device, the data processing device connected to a first network that includes a plurality of networked resources: (Jacobson discloses communications between number of secure zone networks wherein each secure zone network comprises groups of computers (e.g. "file server" which shares functionality with "network resource" as claimed, "time share system, mainframes, supper computer" those share functionality with "data processing device" as claimed): figure 1; column 3, lines 10-19)

A first data structure that specifies at least one security zone from a plurality of security zones that is associated with each of the plurality of networked resources: (Jacobson discloses

“local/remote secure zone Host ID table” which is equivalent to “a first data structure” as claimed used for grouping security zone host devices into a plurality of secure zones; Jacobson discloses the forwarder comprised in the secure bridge determines authorization for source IP address comprised in data packet by associating/mapping/sparing the sources IP address with IP addresses of secure zones in local/remote secure zone Host ID table to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to desired/selected secure destination: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

A second data structure that specifies the respective security zones to which a plurality users of the data processing device may have access: (Jacobson discloses “key tables” which is equivalent to “a second data structure”. The key table comprises information showing the associations between bridge IP addresses, source key variables, destination variables; wherein each of bridge IP address represents for distinct secure zones network. Jacobson discloses after the source IP address included in packet data is determined as authorized in particular secure zone network, the forwarder then retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to desired/selected secure destination: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

A plurality of workstations that configured to execute applications on the data processing device: (Jacobson discloses communications between groups of host computers (e.g.

Art Unit: 2152

mainframes, supper computers, “file servers” those share functionality with network resources as claimed) wherein each group of host computers belongs to different secure zones network, see (column 3, lines 9-18). It would have been obvious to a person of ordinary skill in the art to know that mainframes are often shared by multiple users connected to the mainframes by “terminals” which is interpreted as workstations as claimed

However, Jacobson does not explicitly disclose each of the plurality of security zones represents a distinct level of security sensitivity

In analogous art, Wallent disclose method for grouping web servers into secure zones based on levels of security: (abstract; column 3, lines 20-27)

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wallent’s ideas of grouping servers into secure zones base on levels of security with Jacobson’s system in order to increase security for communication system, see (column 2, lines 37-49)

Regarding claim 2:

Jacobson-Wallent discloses a method as discuss in claim 1, which includes a mainframe computer, and wherein the request is originate on a workstation of the mainframe computer: (Jacobson discloses communications between groups of host computers (e.g. mainframes, supper computers, file servers...etc.) wherein each group of host computers belongs to different secure zones network, see (column 3, lines 9-18). It would have been obvious to a person of ordinary skill in the art to know that mainframes are often shared by multiple users connected to the mainframes by “terminals” which is interpreted as workstations as claimed

Regarding claim 3:

Jacobson-Wallent discloses a method as discuss in claim 2, which further includes the mainframe computer receives the request originated from the user, identifies the plurality of security zones associate with the one for the plurality of resources, and determine if the user is authorized to access to the one of the plurality of resources: (Jacobson's secure system supports for communications between secure zones networks, wherein each of secure zones comprises groups of host computers (e.g. mainframes, supper computers, file server...etc). Jacobson's can be pictured as communications between different secure zones networks, thereby one of secure zones network comprises "mainframes" that share functionality with "mainframe computer" as claimed, obviously a person of ordinary skill in the art to know that mainframes are often shared by multiple users connected to the mainframes by terminals; the other secure zones network comprises "file servers" that shares functionality with "resources" as claimed, see (column 3, lines 9-18). Jacobson further discloses technique of sparing source IP address comprised in packet data with IP addresses of secure zones in local/remote secure zone Host ID table to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to desired/selected secure destination: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

Regarding claim 4:

Jacobson-Wallent discloses a method as discuss in claim 3, which further includes identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises access a data structure the specifies the security zone associated with each

resource in the plurality of resources: (Jacobson discloses technique of using “local/remote secure zone Host ID table” which shares functionality with “a data structure” as claimed to sparing source IP address comprised in packet data with IP addresses of secure zones in the local/remote secure zone Host ID table to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to “desired/selected secure destination” which shares functionality with “each resource” as claimed: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

Regarding claim 5:

Jacobson-Wallent discloses a method as discuss in claim 4, which includes:

“at least one entry in the data structure specifies the security zone associated with a groups of the resources in the plurality of resources”: (Jacobson clearly discloses distinct security zone associated with groups of host computers those could be file server, or mainframes, or supper computers. In this case, the Office interprets host computers would be “file servers” those share functionality with “resources.” So inherently a data structure includes at least one entry specifies the security zone associated with groups of the resources included in Jacobson’s secure system: (column 3, lines 9-18).

“wherein identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises identifying the security zone associated with the most specific entry in the data structure that includes the resource:” (Jacobson discloses technique of using “local/remote secure zone Host ID tables” which could be interpreted as sharing

Art Unit: 2152

functionality with “the data structure” as claimed to sparing source IP address comprised in packet data with IP addresses of secure zones in the local/remote secure zone Host ID table to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to “desired/selected secure destination” which shares functionality with “the resource” as claimed: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

Regarding claims 18 and 23:

Those claims are rejected under rationale of claim 5

Regarding claim 6:

Jacobson-Wallent discloses a method as discuss in claim 1, which further includes the identifying and determining steps are performed within the multi-user system

Jacobson discloses technique of identifying and determining if the source IP address of packet data is authorized in order to forwarding packet data to desired/selected secure destination. Obviously, those techniques can also be applied in “mainframe computer” which shares functionality with “the multi-user system” as claimed: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

Regarding claim 7:

Jacobson-Wallent discloses a method as discuss in claim 1, which includes the message forwarded over the network includes a first user identification associated with the multi-user system but does not include a second user identification associated with the user of the multi-

user system: (Jacobson discloses method for searching combination of Protocol filter table, IP address filter table, identification table in order to determine the authorization for user request; and if the source address/ and destination address does not exist in those tables it will be added into those tables: column 5, lines 1-67; column 6, lines 1-67)

Regarding claim 8:

Jacobson-Wallent discloses a method as discuss in claim 1, which further includes the identifying and determining steps are performed before any data packets associated with message are forwarded over the network: (Jacobson discloses the forwarder comprised in the bridge determines authorization for source IP address comprised in packet data by associating the sources IP address with IP addresses of secure zones in identification tables to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to “desired/selected secure destination” which shares functionality with “an identified security zone”: (Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47)

Regarding claim 9:

Jacobson-Wallent discloses a method as discuss in claim 1, which includes the network is an Internet protocol network: (Jacobson discloses IP protocol filter table: column 5, lines 1-67; column 6, lines 1-67)

Regarding claims 15-17, 20-22 and 28:

Jacobson-Wallent discloses a method as discuss in claims 14,19 and 24 which includes further comprising means for associating a security zone with each of the plurality of resources:

(Jacobson disclose method for grouping security zone host devices into a plurality of secure zones. In the Jacobson system, the network local security bridge includes identification filter table which used to identify if the request transmitted packet is authorized to access one of security zone host device: column 7, lines 1-67; column 8, lines 1-48; column 15, lines 1-67; column 3, lines 42-67, 7-18; figure 1)

Regarding claim 26:

Jacobson-Wallent discloses a method as discuss in claim 25, which includes the first data structure comprises a mapping table that identifies the respective one of the plurality of security zones associated with each of the plurality of networked resources: (Jacobson discloses method using local/ and remote secure zone Host ID tables and keys tables for mapping/ sparing and associating the sources IP address included in packet data with IP addresses of secure zones in identification tables to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to “desired/selected secure destination” which shares functionality with “networked resource” as claimed: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 5, lines 1-67; column 6, lines 1-67)

wherein at least some of the entries in the mapping table are associated with multiple of the plurality of networked resources: (Jacobson: figure 9, figure 10 and figure 11)

Regarding claim 27:

Jacobson-Wallent discloses a method as discuss in claim 26, which includes wherein entries in the mapping table include wildcard characters to specify multiple of the plurality of

networked resources with a single entry in the mapping table: (Jacobson clearly discloses secure zone Host ID tables include plurality of entries and entries characters information e.g. “host IP address, bridge IP address” in table 9; “bridge IP address, source key, dest key” in table 10 those entries characters information represent for “wildcard characters” as claimed: (Jacobson: figure 9, figure 10 and figure 11)

Regarding claim 24:

Jacobson-Wallent discloses a method as discuss in claim 1, which further includes feature of receiving a message over the network from one of the plurality of resources that is addressed to a process running on the multi-user system that is associated with the user: (Jacobson discloses method for bridging secure zone host devices network via using the network security bridges those have ability to transmitt data packets between secure zone host devices e.g. “time sharing system, super computers, mainframes...etc” those share functionality with “the multi-user system therefrom a process associated with user running on” as claimed from distinct secure zones networks; each of network security bridge includes the data packet processor/ and forwarder those receive/ and processe to determine if the data packet is authorized to be transmitted to other secure zones network; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding them to desired/selected secure destination: (Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47)

(10) Response to Argument

a) First, Appellant argues with respect to claims 1, 14 and 19:

Jacobson does not disclose claimed feature of: “identifying a security zone that is associated with a resource to which a message is to be sent”

In reply to Appellant’s arguments:

First, the feature of “identifying a security zone that is associated with a resource to which a message is to be sent” is not disclosed in the rejected claimed; the rejected claim originally claimed as: “identifying a one of the plurality of security zones that is associated with the one of the plurality of resources,” (claim 1, lines 7-8; claim 14, lines 7-8; claim 19, lines 9-10). It is noted that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)

Second, the feature of “identifying a security zone that is associated with a resource to which a message is to be sent” also can be read from the Jacobson as following

Jacobson discloses a method for bridging communications between secure zones networks (e.g. secure zones 108-1, 108-2, 108-3) see (figure 1) through secure bridges; wherein each of secure zones network comprises groups of host computers e.g. mainframes, supper computers, file servers. See (column 3, lines 9-18; abstract). In the Jacobson’s secure system, “the data packets” those share functionality with “messages” as claimed are exchanged between those secure zones networks; each of data packet includes source address, destination address (column 1, lines 40-42) those are used to identifying the secure zones of “the source devices and destination devices” those are shared functionality with “resources” as claimed by

associating/mapping/sparing source IP address comprised in data packet with IP addresses of secure zones in identification tables (abstract, lines 9-14, 17-22; column 1, lines 35-41, 47-51, 55-59) in order to process the data packets (abstract, lines 23-27; column 1, lines 64-66)

b) Second, Appellant argues with respect to claims 1, 14 and 19:

The cited references do not disclose claimed feature of: “identifying one of the plurality of security zones that is associated with the one of the plurality of resources where the resource is the resource that is to receive the message from the user”

In reply to Appellant’s arguments:

This feature is not disclosed in the rejected claimed. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

c) Third, Appellant argues with respect to claims 1, 14 and 19:

Appellant arguments on the differences functionality of filter table and claimed feature of: “identifying a security zone that is associated with a resource”

In reply to Appellant’s arguments:

Jacobson’s system can be pictured as communications between different secure zones networks, thereby one of secure zones network comprises mainframes those are often shared by multiple users connected to the mainframes by terminals; the other secure zones network comprises “file servers” that shares functionality with “resources” as claimed, see (column 3, lines 9-18). Jacobson further discloses a forwarder comprised in the bridges receives and determines authorization for “data packet” which shares functionality with “the message” as claimed by associating/mapping/sparing source IP address comprised in data packet with IP

Art Unit: 2152

addresses of secure zones in identification tables to determine if the data packet is authorized to be forwarded to other secure zone network; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding the encrypted packet data to “desired/selected secure destination” which share functionality with “identified secure zone”: column 7, lines 19-67, 34-44, 54-61; column 8, lines 36-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1; Figure 2, items 220, 230, 236; figure 4b, items 434; 440; figure 4c, item 442; figure 9; figure 11)

d) Fourth, Appellant argues with respect to claims 1, 14 and 19:

Jacobson does not disclose if a user is authorized access to an identified security zone (argument: page 10, lines 14-15)

In reply to Appellant's arguments:

Jacobson discloses a forwarder comprised in the bridge determines authorization for data packet by associating/mapping/sparing “source IP address included in data packet” which represents for user identification with IP addresses of secure zones in identification tables to determine if the data packet is authorized to be forwarded to other secure zones network; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to “desired/selected secure destination” which shares functionality with “an identified security zone”: (Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47)

e) Fifth, Appellant argues with respect to claims 1, 14 and 19:

Jacobson does not disclose claimed feature of: “forwarding a message only if it is determined that the user is authorized access to the identified security zone”

In reply to Appellant’s arguments:

As similar to discussions addressed in section d) above, Jacobson discloses the forwarder comprised in the bridge determines authorization for “source IP address comprised in packet data” which shares functionality with user identification by associating/mapping/sparing the sources IP address with IP addresses of secure zones in identification tables to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to “desired/selected secure destination” which shares functionality with “an identified security zone”: (Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47)

f) Sixth, Appellant argues with respect to claims 1, 14 and 19:

Appellant argues that Jacobson’s library viewing/ and or installing do nothing with claimed feature of: “receiving a request from a use of multi-use system to transmit a message over a network”

In reply to Appellant’s arguments:

The claimed feature of “receiving a request from a user of multi-use system to transmit a message over a network” is not rejected by applying viewing/ and or installing in Jacobson’s library in the Office Action

This claimed feature is taught by the Jacobson see (Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-

47; figure 3). In Jacobson's secure system, thereby communications between secure zones networks (e.g. 108-1 to 108-3) see (figure 1) are implemented and controlled by local/ and remote secure bridges; each of secure zone networks comprises group of host computers e.g. "mainframes, supper computers" those share functionality with "multi-user system" as claimed and file servers, see (column 3, lines 9-18). Jacobson's secure system can be pictured as one of secure zones network comprises mainframes that are often shared by multiple users connected to the mainframes by terminals for establishing communications with other mainframes users, supper computers, or file servers in other secure zones networks.

g) Seventh, Appellant argues with respect to claim 24:

Appellant argues that the Office Action does not identify what elements of Jacobson correspond to the recited feature of "process running on the multi-user system" or associated "user"

In reply to Appellant's arguments:

As similar to discussions addressed in section g) Jacobson's secure system supports for communications between numbers of secure zones networks; wherein each secure zones network comprises group of computer hosts e.g. "time sharing system, super computers, mainframes...etc." those share functionality with "the multi-user system as claimed; obviously mainframes are often "shared" which shares functionality with "process" as claimed by multiple users connected to the mainframes by terminals, see (column 3, lines 9-18)

h) Eighth, Appellant argues with respect to claim 25:

Regarding to rejections for claimed feature of “plurality of workstations that are configured to execute applications on the data processing device”. Application indicates that the host devices of Jacobson are not configured to execute application one each other

In reply to Appellant’s arguments:

As similar to discussions addressed in section f) Jacobson’s secure system supports for communications between numbers of secure zones networks; wherein each secure zones network comprises group of computer hosts e.g. “time sharing system, super computers, mainframes...etc.” those share functionality with “the data processing device” as claimed; obviously mainframes are often “shared” which shares functionality with “executing application” as claimed by multiple users connected to the mainframes by “terminals” that share functionality with “workstations” as claimed, see (column 3, lines 9-18)

i) Ninth, Appellant argues with respect to claim 25:

The Host ID table of Jacobson is not same as a first data structure to mapping network resources to particular security zones

In reply to Appellant’s arguments:

First, the feature of “a first data structure to mapping the network resources to particular security zones” was not disclosed in rejected claim. It is noted that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)

Second, the reasons for associating “local/remote secure zone Host ID tables” with the first data structure” as claimed in the Office Action because the local/remote secure Host Id tables comprises information showing relationships between “host IP address” which represents

for “network resources” as claimed and bridge IP address, see (figure 9); Jacobson teaches that the secure bridges are capable to manage/ establish communications between secure zones 108-1 to 108-3 network/ and secure sides, see (figure 1; figure 5; column 7, lines 25-34; column 3, lines 31-56). Also, Jacobson clearly demonstrates (through figure 9, column 7, lines 25-34) a method of using “local/remote secure zone Host ID tables” to specifying the associations between secure zones (e.g. 108-1 to 108-3) and “remote secure hosts” those share functionality with “resources” as claimed by mapping/sparing the sources IP address included in data packet with IP addresses in local/remote secure zone Host ID tables

j) Tenth, Appellant argues with respect to claim 25:

Jacobson does not disclose second data structure as claimed because the authorization table does not specify the respective security zones to which a use may have access

In reply to Appellant’s arguments:

The feature of “second data structure specifies the respective security zones to which a user may have access” was not disclosed in the rejected claim

k) Eleventh, Appellant argues with respect to claim 2:

regarding claimed feature of “the multi-user system comprises a mainframe computer, and wherein the request is originated on a workstation of mainframe computer”

In reply to Appellant’s arguments:

Jacobson’s secure system can be pictured as one of secure zones network comprises mainframes that are often shared by multiple users connected to the mainframes by “terminals” those share functionality with “workstations” as claimed for establishing communications with other mainframes users, supper computers, or file servers in other secure zones networks, see

Art Unit: 2152

(column 3, lines 9-18; column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; figure 3)

1) Twelfth, Appellant argues with respect to claims 3-4:

regarding claimed feature of “the mainframe computer receives the request originated from the user, identifies the plurality of security zones associate with the one for the plurality of resources, and determine if the user is authorized to access to the one of the plurality of resources”

In reply to Appellant’s arguments:

Jacobson’s secure system supports for communications between secure zones networks, wherein each of secure zones network comprises groups of host computers (e.g. mainframes, supper computers, file server...etc). Jacobson’s system can be pictured as communications between different secure zones networks, thereby one of secure zones network comprises mainframes, obviously the mainframes are often shared by multiple users connected to the mainframes by terminals; the other secure zones network comprises “file servers” that shares functionality with “resources” as claimed, see (column 3, lines 9-18). Jacobson further discloses technique of sparing/mapping source IP address comprised in data packet with IP addresses in local/remote secure zone Host ID tables in order to determine if the data packet is authorized to be forwarded to other secure zones network; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding the data packet to desired/selected secure destination: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

m) Thirteenth, Appellant argues with respect to claims 3-4:

regarding claimed feature of “identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises access a data structure the specifies the security zone associated with each resource in the plurality of resources”

In reply to Appellant’s arguments:

Jacobson discloses “the local/remote secure Host Id tables” that share functionality with “a data structure” as claimed comprises information showing relationships between “host IP addresses” which represents for “resources” as claimed and bridge IP address, see (figure 9); Jacobson teaches that the secure bridges are capable to manage/ establish communications between secure zones networks 108-1 to 108-3/ and secure sides, see (figure 1; figure 5; column 7, lines 25-34; column 3, lines 31-56). Also, Jacobson clearly demonstrates (through figure 9, column 7, lines 25-34) a method of using “local/remote secure zone Host ID tables” to specifying the associations between secure zones (e.g. 108-1 to 108-3) and “remote secure hosts” those share functionality with “resources” as claimed

n) Fourteenth, Appellant argues with respect to claims 5, 18 and 23:

The Office action fails to provide citations and explanation for limitations of the claim

In reply to Appellant’s arguments:

The citations and explanations are provided as following:

“at least one entry in the data structure specifies the security zone associated with a groups of the resources in the plurality of resources”: (Jacobson clearly discloses distinct security zones (e.g. secure zone 108-03, 108-01, 108-2) associated with groups of host computers those could be file servers, or mainframes, or supper computers. In this case, the Office interprets host

computers would be “file servers” those share functionality with “resources” as claimed. So inherently a data structure “e.g. local/remote secure zone Host ID tables” includes at least one entry specifies the security zone associated with groups of the resources included in Jacobson’s secure system: (figure 1; abstract; column 3, lines 9-18).

“wherein identifying the one of the plurality of security zones associated with the one of the plurality of resources comprises identifying the security zone associated with the most specific entry in the data structure that includes the resource:” (Jacobson discloses technique of using “local/remote secure zone Host ID tables” which shares functionality with “the data structure” as claimed to sparing/mapping source IP address comprised in data packet with IP addresses of secure zones in the local/remote secure zone Host ID tables to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding it to “desired/selected secure destination” which shares functionality with “the resource” as claimed: Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

o) Fifteenth, Appellant argues with respect to claim 6:

The Office action fails to provide citations and explanation for limitation of the claim: “identifying and determining steps are performed within the multi-user system”

In reply to Appellant’s arguments:

The citations and explanations are provided as following:

Jacobson clearly discloses technique of identifying and determining if the source IP address of packet data is authorized in order to forwarding data packet to desired/selected secure

destination. Obviously, those techniques can also be applied in any environments e.g. mainframe computer: (Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47; column 3, lines 42-67, 7-18; figure 9; figure 1)

p) Sixteenth, Appellant argues with respect to claim 8:

The Office action fails to provide citations and explanation for limitations of the claim: “identifying and determining steps are performed before any data packets associated with the message are forward over the network”

In reply to Appellant’s arguments:

The citations and explanations are provided as following:

Jacobson discloses the forwarder comprised in the secure bridge determines authorization for source IP address comprised in data packet by associating/mapping/sparing the sources IP address with IP addresses in secure zones in identification tables to determine if the source IP address is authorized; if so, then the forwarder retrieves decryption key/ encryption key from key tables to decrypt/ encrypt the packet data prior forwarding the data packet to “desired/selected secure destination” which shares functionality with “an identified security zone”: (Column 7, lines 19-67; column 8, lines 50-61; column 9, lines 1-7, 16-24; column 10, lines; column 11, lines 45-67; column 12, lines 1-47)

q) Eighteenth, Appellant argues with respect to claim 26:

Jacobson does not disclose claimed feature: “the identified tables identify the respective security zones that are associated with each of the network resources”

In reply to Appellant’s arguments:

Jacobson clearly discloses distinct security zones (e.g. secure zone 108-03, 108-01, 108-2) associated with groups of host computers those could be file server, or mainframes, or super computers. In this case, the Office interprets host computers would be “file servers” those share functionality with “resources” as claimed. Jacobson further discloses “the local/remote secure Host Id tables” that share functionality with “identified tables” as claimed comprises information showing relationships between “host IP addresses” which represents for “network resources” as claimed and “bridge IP address” those represents for secure zones, see (figure 9), such as, the secure bridges are capable to manage/ establish communications between secure zones network i.e. 108-1 to 108-3/ and secure sides, see (figure 1; figure 5; column 7, lines 25-34; column 3, lines 31-56). Also, Jacobson clearly demonstrates (through figure 9, column 7, lines 25-34) a method of using “local/remote secure zone Host ID tables” to specifying the associations between secure zones (e.g. 108-1 to 108-3) and “remote secure hosts” those share functionality with “network resources” as claimed

r) Nineteenth, Appellant argues with respect to claim 26:

Jacobson does not disclose claimed feature: “the entries in the tables”

In reply to Appellant’s arguments:

Jacobson clearly discloses secure zone Host ID tables include plurality of entries:

(Jacobson: figure 9, figure 10 and figure 11)

r) Twenty, Appellant argues with respect to claim 27:

Regarding “wildcard characters” feature

In reply to Appellant’s arguments:

Jacobson clearly discloses secure zone Host ID tables include plurality of entries and entries characters information e.g. "host IP address, bridge IP address" in table 9; "bridge IP address, source key, dest key" in table 10 those entries characters information represent for "wildcard characters" as claimed: (Jacobson: figure 9, figure 10 and figure 11)

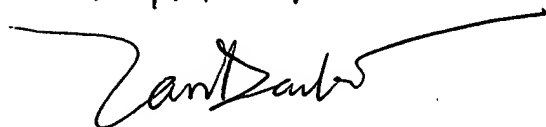
(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusions

For the above reasons, it is believed that the rejections should be sustained.

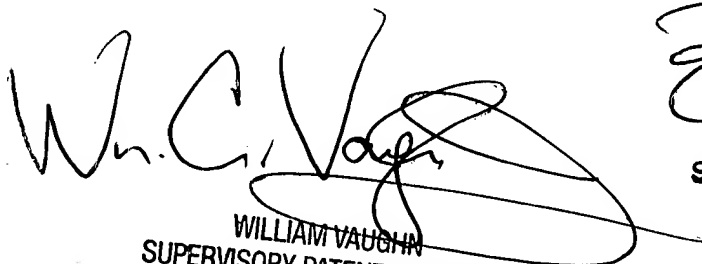
Respectfully submitted,
10/10/2007



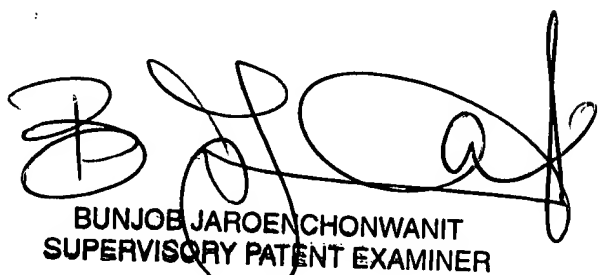
Lan-Dai, Truong

Conferees:

Bunjob Jaroenchonwanit
Supervisory Patent Examiner
Technology Center 2100



WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
10/12/07



BUNJOB JAROENCHONWANIT
SUPERVISORY PATENT EXAMINER
10/11/7